

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

JONATHAN HUNTER, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

FRED HUTCHINSON CANCER CENTER, a  
Washington Nonprofit Corporation,

Defendant.

NO.

**COMPLAINT - CLASS ACTION**

**CLASS ACTION COMPLAINT**

Plaintiff Jonathan Hunter (“Plaintiff”), individually, and on behalf of all others similarly situated, brings this action against Defendant Fred Hutchinson Cancer Center (“Defendant” or “Fred Hutch”). Plaintiff brings this action by and through his attorneys, and alleges, based upon personal knowledge as to his own actions, and based upon his information and belief and reasonable investigation by his counsel as to all other matters, as follows.

**I. INTRODUCTION**

1. Fred Hutch is a cancer research institute based in Seattle, Washington, and is a preeminent leader in cancer care as well as cancer and infectious disease research. Fred Hutch operates eleven clinical care sites in Washington that provide medical oncology, infusion,

1 radiation, proton therapy and related services to cancer patients. Fred Hutch treats thousands of  
2 patients each year; in 2022, Fred Hutch provided care to over 50,000 individuals diagnosed with  
3 and at risk for cancer.<sup>1</sup>

4 2. As part of its operations, Fred Hutch collects, maintains, and stores highly  
5 sensitive personal and medical information belonging to its patients, including, but not limited  
6 to: first and last names, addresses, Social Security numbers, dates of birth (collectively,  
7 “personally identifying information” or “PII”), health insurance information, information  
8 concerning patients’ medical history, mental or physical conditions, and medical diagnosis and  
9 treatment (collectively, “private health information” or “PHI”) (PII and PHI collectively are  
10 “Private Information”).

11 3. On or about November 19, 2023, Fred Hutch detected an incident in which  
12 unauthorized cybercriminals accessed information on its clinical network (the “Data Breach”).  
13 Upon information and belief, the cybercriminals accessed and stole Private Information  
14 belonging to Plaintiff and Class members. Fred Hutch asserts that when it discovered the  
15 unauthorized access, it “immediately notified federal law enforcement and engaged a leading  
16 forensic security firm to investigate and contain the incident,” and it also took its “clinical  
17 network offline and implemented additional information technology security protocols.”<sup>2</sup>

18 4. Since the incident, hundreds of Fred Hutch patients have received threatening  
19 emails from cybercriminals. In these emails, cybercriminals claim that information for 800,000  
20 patients was stolen in the Data Breach—including names, social security numbers, medical and  
21

---

22 <sup>1</sup> *About Fred Hutch: 2022 Annual Report, Fred Hutch Cancer Center,*  
23 <https://www.fredhutch.org/en/about/about-the-hutch/annual-report.html> (last visited Dec. 7, 2023).

24 <sup>2</sup> *Update on Data Security Incident, Fred Hutch Cancer Center,*  
<https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html>  
(last visited Dec. 7, 2023).

1 insurance information, lab results and more—and demands payment to prevent the sale of that  
2 data.<sup>3</sup>

3 5. On or about December 6, 2023, Fred Hutch sent an email to all current and former  
4 patients notifying them of the Data Breach and instructing all patients to “remain vigilant to  
5 protect against potential fraud and/or identity theft by, among other things, reviewing your  
6 account statements and monitoring credit reports closed.”<sup>4</sup>

7 6. As Fred Hutch stored and handled such highly-sensitive Private Information, it  
8 had a duty and obligation to safeguard this information and prevent unauthorized third parties  
9 from accessing this data.

10 7. Ultimately, Fred Hutch failed to fulfill these obligations as unauthorized  
11 cybercriminals breached Fred Hutch’s information systems and databases, and upon information  
12 and belief, stole vast quantities of Private Information belonging Plaintiff and Class members.  
13 This breach—and the successful compromise of Private Information—were direct, proximate,  
14 and foreseeable results of multiple failings on the part of Fred Hutch.

15 8. The Data Breach occurred because Fred Hutch inexcusably failed to implement  
16 reasonable security protections to safeguard its information systems and databases. Fred Hutch  
17 also inexcusably failed to timely detect this Data Breach. And before the breach occurred, Fred  
18 Hutch failed to inform the public that its data security practices were deficient and inadequate.  
19 Had Plaintiff and the Class members been made aware of this fact, they would have never  
20 provided such information to Fred Hutch.

---

21  
22 <sup>3</sup> Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*,  
23 KUOW (Dec. 6, 2023), [https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-](https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack)  
24 [after-fred-hutch-cyberattack](https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack) (last visited Dec. 7, 2023).

<sup>4</sup> This Email Notice, which contains information regarding the data security breach incident, is  
attached as **Exhibit A**.



12. Defendant Fred Hutchinson Cancer Center is a Washington nonprofit corporation with its principal place of business located at 1100 Fairview Ave. N., Seattle, WA 98109-1024. Fred Hutch conducts business in this County and throughout Washington State. Fred Hutch provides medical services and treatments to patients at its 11 clinical sites located across the Puget Sound region. Its main campus—and the home of its cancer research center—is in the South Lake Union area of Seattle, Washington.

### III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

14. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in Washington; it is registered with the Secretary of State in Washington as a Washington nonprofit corporation; it maintains its headquarters in Washington; and committed tortious acts in Washington.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Defendant has the most significant contacts.

### IV. FACTUAL ALLEGATIONS

#### A. Fred Hutch – Background

16. In April 2022, Fred Hutchinson Cancer Center was created by way of a merger of Fred Hutchinson Cancer Research Center with the Seattle Cancer Care Alliance (SCCA). The

1 result of unifying these research and patient care entities was the creation of a unified adult cancer  
2 research and care center that is clinically integrated with University of Washington (UW)  
3 Medicine and UW Medicine's cancer program. The purpose of this merger was to integrate  
4 scientific endeavors and clinical care to ensure patients have access to the most innovative care.  
5 As a result of the restructuring, Fred Hutch now serves as UW Medicine's cancer program.<sup>5</sup>

6 17. Fred Hutch is an independent organization that specializes in cancer care as well  
7 as cancer and infectious disease research. Fred Hutch operates through its campus headquarters  
8 in Seattle and its eleven clinical care sites across the Puget Sound region of Washington, which  
9 provide medical oncology, infusion, radiation, proton therapy and related services to cancer  
10 patients.

11 18. In order to provide healthcare and related research services, Fred Hutch collects,  
12 maintains, and stores the highly sensitive PII and PHI provided by its current and former patients,  
13 including but not limited to: first and last name, Social Security number, date of birth, health  
14 insurance policy number, and information about medical history, mental or physical condition,  
15 or medical diagnosis or treatment.

16 19. As a result of Fred Hutch's relationship with UW Medicine, its computer systems  
17 and networks also house some University of Washington Medicine patient data.<sup>6</sup>

18 20. On information and belief, Fred Hutch failed to implement necessary data security  
19 to protect Plaintiff's and Class members' Private Information at the time of the Data Breach. This  
20

---

21 <sup>5</sup> *Hutch News Stories: Fred Hutch and Seattle Cancer Care Alliance unite, reshape relationship*  
22 *with UW Medicine*, Fred Hutch Cancer Center (Apr. 1, 2022),  
<https://www.fredhutch.org/en/news/center-news/2022/04/fred-hutch-scca-restructure.html> (last visited  
23 Dec. 7, 2023).

24 <sup>6</sup> Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*,  
KUOW (Dec. 6, 2023), [https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-](https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack)  
[after-fred-hutch-cyberattack](https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack) (last visited Dec. 7, 2023).

1 failure resulted in cybercriminals accessing the Private Information of Fred Hutch's current and  
 2 former patients—Plaintiff and Class members.

3 21. Current and former patients of Fred Hutch, such as Plaintiff and Class members,  
 4 made their Private Information available to Fred Hutch with the reasonable expectation that any  
 5 entity with access to this information would keep that sensitive and personal information  
 6 confidential and secure from illegal and unauthorized access. And, in the event of any  
 7 unauthorized access, these entities would provide them with prompt and accurate notice.

8 22. This expectation was objectively reasonable and based on an obligation imposed  
 9 on Fred Hutch by statute, regulations, industry standard, and standards of general due care.

10 23. Unfortunately for Plaintiff and Class members, Fred Hutch failed to carry out its  
 11 duty to safeguard sensitive Private Information and provide adequate data security. As a result,  
 12 it failed to protect Plaintiff and Class members from having their Private Information accessed  
 13 and stolen during the Data Breach.

#### 14 **B. The Data Breach**

15 24. On November 19, 2023, Fred Hutch detected that cybercriminals had engaged in  
 16 unauthorized activity on its clinical network. Upon detecting the incident, Fred Hutch engaged a  
 17 specialized third-party forensic security firm to assist with containing its network and  
 18 investigating the extent of unauthorized activity.<sup>7</sup> The cybersecurity incident specifically  
 19 involved Fred Hutch's clinical systems, but those systems also house University of Washington  
 20 Medicine patient data.<sup>8</sup>

21  
 22 <sup>7</sup> Update on Data Security Incident, Fred Hutch Cancer Center,  
<https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html>  
 (last visited Dec. 7, 2023).

23 <sup>8</sup> Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*,  
 24 KUOW (Dec. 6, 2023), <https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack> (last visited Dec. 7, 2023).

1           25.     Upon information and belief, cybercriminals successfully breached Fred Hutch's  
2 systems in the Data Breach and accessed Private Information of current and former Fred Hutch  
3 patients, including their first and last name, date of birth, Social Security number, medical  
4 information, diagnosis and treatment information, and health insurance information.<sup>9</sup>

5           26.     Immediately following the Data Breach, hundreds of Fred Hutch patients have  
6 received threatening emails from cybercriminals related to the Data Breach. "The emails claim  
7 that information for 800,000 Fred Hutch patients was compromised in the Data Breach, including  
8 names, social security numbers, medical and insurance information, lab results and more. The  
9 cybercriminals sending these emails demand that patients pay them to prevent the sale of that  
10 data."<sup>10</sup>

11           27.     The threatening emails state: "If you are reading this, your data has been stolen  
12 and will soon be sold to various data brokers and black markets to be used in fraud and other  
13 criminal activities." The threatening emails also include specific examples of the personal data  
14 stolen and exposed for the individual recipient of the email, including their name, address, and  
15 patient record number, and even contain medical information. As of December 6, 2023, at least  
16 300 patients have contacted Fred Hutch after receiving one of these threatening emails.

17           28.     Following the Data Breach and commencement of its investigation, Fred Hutch  
18 took our clinical network offline and implemented additional information technology security  
19 protocols.<sup>11</sup>

---

22           <sup>9</sup> *Id.*

23           <sup>10</sup> *Id.*

24           <sup>11</sup> *Update on Data Security Incident*, Fred Hutch Cancer Center,  
<https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html>  
(last visited Dec. 7, 2023).

1           29. On December 6, 2023, Fred Hutch sent a data breach notice to all current and  
 2 former patients notifying them of the Data Breach and the risk of harm those individuals now  
 3 face as a result of the Data Breach.<sup>12</sup>

4 **C. Fred Hutch's Failure to Protect Its Patient's Private Information**

5           30. Fred Hutch collects and maintains vast quantities of Private Information  
 6 belonging to Plaintiff and Class members as part of its normal operations as a healthcare service  
 7 provider. The data breach occurred as a direct, proximate, and foreseeable result of multiple  
 8 failings on the part of Fred Hutch.

9           31. Fred Hutch inexcusably failed to implement reasonable security protections to  
 10 safeguard its information systems and databases.

11           32. Fred Hutch failed to inform the public that its data security practices were  
 12 deficient and inadequate. Had Plaintiff and the Class Members been aware that Fred Hutch did  
 13 not have adequate safeguards in place to protect such sensitive Private Information, they would  
 14 never have provided such information to Fred Hutch.

15           33. Plaintiff's and Class members' Private Information was accessed and acquired by  
 16 cybercriminals for the express purpose of misusing the data. They face the real, immediate, and  
 17 likely danger of identity theft and misuse of their Private Information. And this can, and in some  
 18 circumstances already has, caused irreparable harm to their personal, financial, reputational, and  
 19 future well-being. This harm is even more acute because much of the stolen Private Information,  
 20 such as healthcare data, is immutable.

21  
 22  
 23  
 24 <sup>12</sup> Exhibit A.

**D. Data Breaches Pose Significant Threats**

34. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, are an invaluable commodity and a frequent target of hackers.

35. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.<sup>13</sup> The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just eight shy of the record of 715 set in 2021, and still double that of the number of similar such compromises in 2017.<sup>14</sup>

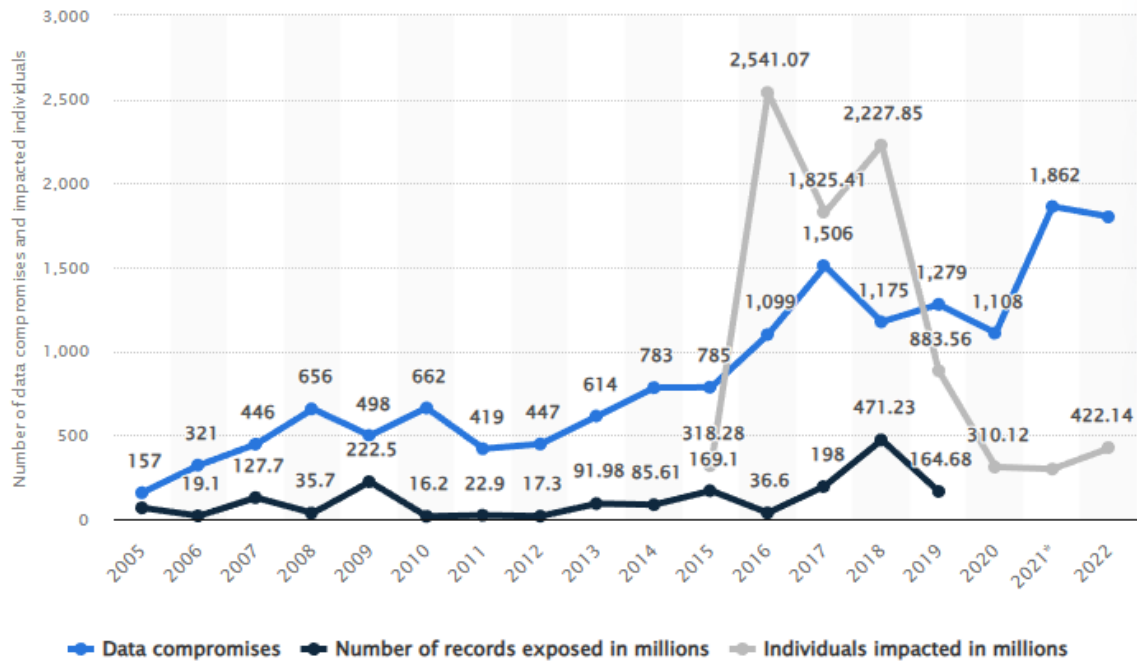
36. Statista, a German entity that collects and markets data relating to data breach incidents and their consequences, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005; it reported 157 compromises in 2005, to a peak of 1,862 in 2021, to 2022's total of 1,802.<sup>15</sup> The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.<sup>16</sup>

<sup>13</sup> 2022 End of Year Data Breach Report, Identity Theft Resource Center at 6 (Jan. 25, 2023), available at [https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm\\_source=press+release&utm\\_medium=web&utm\\_campaign=2022+Data+Breach+Report](https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report) (last accessed Dec. 7, 2023).

<sup>14</sup> 2022 Healthcare Data Breach Report, The HIPAA Journal (Jan. 24, 2023), available at <https://www.hipaajournal.com/2022-healthcare-data-breach-report/> (last accessed Dec. 7, 2023).

<sup>15</sup> Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022, Statista, available at <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/> (last accessed Dec. 7, 2023).

<sup>16</sup> *Id.*



37. This stolen Private Information is then routinely traded on dark web black markets as a simple commodity.<sup>17</sup>

38. Armed with just a name and Social Security Number, criminals can fraudulently take out loans under a victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>18</sup>

<sup>17</sup> Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (Nov. 15, 2023), available at <https://cybernews.com/security/whats-your-identity-worth-on-dark-web/> (last accessed Dec. 7, 2023).

<sup>18</sup> United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration at 1 (July 2021), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Dec. 7, 2023).

39. The problems associated with a compromised Social Security Number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.<sup>19</sup>

40. The most sought after and expensive pieces of information on the dark web are stolen medical records, which command prices from \$250 to \$1,000 each.<sup>20</sup> Medical records are considered the most valuable because—unlike credit cards, which can easily be canceled, and social security numbers, which can be changed—medical records contain “a treasure trove of unalterable data points, such as a patient’s medical and behavioral health history and demographics, as well as their health insurance and contact information.”<sup>21</sup> With this bounty of ill-gotten information, cybercriminals can steal victims’ public and insurance benefits and bill medical charges to victims’ accounts.<sup>22</sup> Cybercriminals can also change the victims’ medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical

---

<sup>19</sup> *Id.*

<sup>20</sup> Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), available at <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web> (last accessed Dec. 7, 2023).

<sup>21</sup> *Id.*

<sup>22</sup> *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at <https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare> (last accessed Dec. 7, 2023); see also Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), available at <https://www.consumerreports.org/health/medical-identity-theft-a1699327549/> (last accessed Dec. 7, 2023).

1 treatment.<sup>23</sup> Victims of medical identity theft could even face prosecution for drug offenses when  
 2 cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.<sup>24</sup>

3 41. The wrongful use of compromised medical information is known as medical  
 4 identity theft, and the damage resulting from medical identity theft is routinely far more serious  
 5 than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an  
 6 average of \$13,500 to resolve problems arising from medical identity theft and there are currently  
 7 no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's  
 8 liability for fraudulent credit card charges is capped at \$50).<sup>25</sup> It is also "considerably harder" to  
 9 reverse the damage from the consequences of medical identity theft.<sup>26</sup>

10 42. Instances of medical identity theft have grown exponentially over the years, from  
 11 approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold  
 12 increase in the crime.<sup>27</sup>

13 43. In light of the dozens of high-profile health and medical information data breaches  
 14 that have been reported in recent years, entities like Fred Hutch—which are charged with  
 15 maintaining and securing patient PII and PHI—should know the importance of protecting that  
 16 information from unauthorized disclosure. Indeed, Fred Hutch knew, or certainly should have  
 17 known, of the recent and high-profile data breaches in the health care industry: UnityPoint  
 18  
 19  
 20

---

21 <sup>23</sup> *Id.*

22 <sup>24</sup> *Id.*

23 <sup>25</sup> Medical Identity Theft, AARP (March 25, 2022), *available at*  
<https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html> (last accessed Dec. 7,  
 24 2023).

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

1 Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare,  
2 Anthem, Premera Blue Cross, and many others.<sup>28</sup>

3 44. In addition, the Federal Trade Commission (“FTC”) has brought dozens of cases  
4 against companies that have engaged in unfair or deceptive practices involving inadequate  
5 protection of consumers’ personal data, including recent cases concerning health-related  
6 information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized  
7 these enforcement actions to place companies like Fred Hutch on notice of their obligation to  
8 safeguard customer and patient information.<sup>29</sup>

9 45. Given the nature of Fred Hutch’s Data Breach, it is foreseeable that the  
10 compromised Private Information has been or will be used by hackers and cybercriminals in a  
11 variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class  
12 members’ Private Information can easily obtain Plaintiff’s and Class members’ tax returns or  
13 open fraudulent credit card accounts in their names.

14 46. The information compromised in the Data Breach is significantly more valuable  
15 than the loss of, for example, credit card information, because credit card victims can cancel or  
16 close credit and debit card accounts.<sup>30</sup> The information compromised in this Data Breach is  
17 impossible to “close” and difficult, if not impossible, to change.

18 47. To date, Fred Hutch has not offered its patients identity theft monitoring services.  
19

---

20 <sup>28</sup> See, e.g., *Healthcare Data Breach Statistics*, HIPAA Journal, available at:  
21 <https://www.hipaajournal.com/healthcare-data-breach-statistics> (last accessed Dec. 7, 2023).

<sup>29</sup> See, e.g., *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C.  
22 Jan. 26, 2021).

<sup>30</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, *Forbes* (Mar 25, 2020), available at <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1> (last accessed Dec. 7, 2023); see also *Why Your Social Security Number Isn’t as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at <https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/> (last accessed Dec. 7, 2023).

48. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Fred Hutch failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Fred Hutch's failure to implement or maintain adequate data security measures for its current and former patients.

#### **E. Fred Hutch Had a Duty and Obligation to Protect Private Information**

49. Fred Hutch has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and PHI. And third, Fred Hutch imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class members provided, and Fred Hutch obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

##### **1. HIPAA Requirements and Violation**

50. HIPAA requires, among other things, that Covered Entities and Business Associates implement and maintain policies, procedures, systems, and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI; protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI; regularly review access to data bases containing protected information; and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

1           51.     HIPAA, as applied through federal regulations, also requires private information  
2 to be stored in a manner that renders it, “unusable, unreadable, or indecipherable to unauthorized  
3 persons through the use of a technology or methodology. . .” 45 CFR § 164.402.

4           52.     The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires Fred  
5 Hutch to provide notice of the Data Breach to each affected individual “without unreasonable  
6 delay and *in no case later than 60 days following discovery of the breach.*” (emphasis added).

7           53.     Upon information and belief, Fred Hutch failed to implement and/or maintain  
8 procedures, systems, and safeguards to protect the PII and PHI belonging to Plaintiff and the  
9 Class from unauthorized access and disclosure.

10          54.     Upon information and belief, Fred Hutch’s security failures include, but are not  
11 limited to:

- 12           a.     Failing to maintain an adequate data security system to prevent data loss;
- 13           b.     Failing to mitigate the risks of a data breach and loss of data;
- 14           c.     Failing to ensure the confidentiality and integrity of electronic protected health  
15 information Fred Hutch creates, receives, maintains, and transmits in violation  
16 of 45 CFR 164.306(a)(1);
- 17           d.     Failing to implement technical policies and procedures for electronic  
18 information systems that maintain electronic protected health information to  
19 allow access only to those persons or software programs that have been granted  
20 access rights in violation of 45 CFR 164.312(a)(1);
- 21           e.     Failing to implement policies and procedures to prevent, detect, contain, and  
22 correct security violations in violation of 45 CFR 164.308(a)(1);
- 23           f.     Failing to identify and respond to suspected or known security incidents;
- 24           g.     Failing to mitigate, to the extent practicable, harmful effects of security  
incidents that are known to the covered entity, in violation of 45 CFR  
164.308(a)(6)(ii);

- 1 h. Failing to protect against any reasonably-anticipated threats or hazards to the  
2 security or integrity of electronic protected health information, in violation of  
3 45 CFR 164.306(a)(2);
- 4 i. Failing to protect against any reasonably anticipated uses or disclosures of  
5 electronic protected health information that are not permitted under the privacy  
6 rules regarding individually identifiable health information, in violation of 45  
7 CFR 164.306(a)(3);
- 8 j. Failing to ensure compliance with HIPAA security standard rules by Fred  
9 Hutch's workforce, in violation of 45 CFR 164.306(a)(94); and
- 10 k. Impermissibly and improperly using and disclosing protected health  
11 information that is and remains accessible to unauthorized persons, in violation  
12 of 45 CFR 164.502, *et seq.*

13 55. Upon information and belief, Fred Hutch also failed to store the information it  
14 collected in a manner that rendered it "unusable, unreadable, or indecipherable to unauthorized  
15 persons," in violation of 45 CFR § 164.402.

16 56. Because Fred Hutch has failed to comply with HIPAA, while monetary relief may  
17 cure some of Plaintiff's and Class members' injuries, injunctive relief is also necessary to ensure  
18 Fred Hutch's approach to information security is adequate and appropriate going forward. Fred  
19 Hutch still maintains the PHI and other highly sensitive PII of its current and former patients,  
20 including Plaintiff and Class members. Without the supervision of the Court through injunctive  
21 relief, Plaintiff's and Class members' Private Information remains at risk of subsequent data  
22 breaches.

## 23 2. FTC Act Requirements and Violations

24 57. The FTC has promulgated numerous guides for businesses that highlight the  
importance of implementing reasonable data security practices. According to the FTC, the need  
for data security should be factored into all business decision making. Indeed, the FTC has  
concluded that a company's failure to maintain reasonable and appropriate data security for

1 consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the  
 2 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham*  
 3 *Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

4 58. In 2016, the FTC updated its publication, *Protecting Personal Information: A*  
 5 *Guide for Business*, which established guidelines for fundamental data security principles and  
 6 practices for business.<sup>31</sup> The guidelines note businesses should protect the personal information  
 7 that they keep; properly dispose of personal information that is no longer needed; encrypt  
 8 information stored on computer networks; understand their network's vulnerabilities; and  
 9 implement policies to correct security problems.<sup>32</sup> The guidelines also recommend that  
 10 businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all  
 11 incoming traffic for activity indicating someone is attempting to hack the system; watch for large  
 12 amounts of data being transmitted from the system; and have a response plan ready in the event  
 13 of a breach.<sup>33</sup> Fred Hutch clearly failed to do any of the foregoing, as evidenced by the Data  
 14 Breach itself.

15 59. The FTC further recommends that companies not maintain PII longer than is  
 16 needed for authorization of a transaction, limit access to sensitive data, require complex  
 17 passwords to be used on networks, use industry-tested methods for security, monitor the network  
 18 for suspicious activity, and verify that third-party service providers have implemented reasonable  
 19 security measures.

---

22 <sup>31</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October  
 23 2016), available at [https://www.ftc.gov/business-guidance/resources/protecting-personal-information-](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business)  
 24 [guide-business](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business) (last accessed Dec. 7, 2023).

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

1           60.     The FTC has brought enforcement actions against businesses for failing to  
2 adequately and reasonably protect customer data by treating the failure to employ reasonable and  
3 appropriate measures to protect against unauthorized access to confidential consumer data as an  
4 unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify  
5 the measures businesses must take to meet their data security obligations.

6           61.     Additionally, the FTC Health Breach Notification Rule obligates companies that  
7 suffered a data breach to provide notice to every individual affected by the data breach, as well  
8 as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

9           62.     As evidenced by the Data Breach, Fred Hutch failed to properly implement basic  
10 data security practices. Fred Hutch's failure to employ reasonable and appropriate measures to  
11 protect against unauthorized access to Plaintiff's and Class members' Private Information  
12 constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

13           63.     Fred Hutch was fully aware of its obligation to protect the Private Information of  
14 its current and former patients, including Plaintiff and Class members, as Fred Hutch is a  
15 sophisticated and technologically savvy healthcare group that relies extensively on technology  
16 systems and networks to maintain its practice, including storing its patients' PII, protected health  
17 information, and medical information to operate its business.

18           64.     Fred Hutch had and continues to have a duty to exercise reasonable care in  
19 collecting, storing, and protecting the Private Information of Plaintiff and the Class from the  
20 foreseeable risk of a data breach. The duty arises out of the special relationship that exists  
21 between Fred Hutch and Plaintiff and Class members. Fred Hutch alone had the exclusive ability  
22 to implement adequate security measures to its cyber security network to secure and protect  
23 Plaintiff's and Class members' Private Information.

### 3. Industry Standards and Noncompliance

65. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

66. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Fred Hutch include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Fred Hutch failed to follow some or all these industry best practices.

67. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Fred Hutch failed to follow these cybersecurity best practices.

68. Fred Hutch should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. Upon information and belief, Fred Hutch failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

1                                   **4. Fred Hutch’s Own Stated Policies and Promises**

2           70. Fred Hutch claims that “at Fred Hutchinson Cancer Center, we take the privacy  
3 of our patients’ health care information seriously.”<sup>34</sup>

4           71. Fred Hutch’s own published privacy policy states that: “We are required by law  
5 to maintain the privacy and security of your protected health information.”<sup>35</sup> The Privacy Policy  
6 further promises that Fred Hutch “will not use or share your information other than as described  
7 here unless you tell us we can in writing.”<sup>36</sup> The only stated exceptions to the requirement for a  
8 patient’s written consent are for treatment, for payment, for running Fred Hutch’s organization,  
9 to comply with certain laws, for certain research projects, for organ and tissue donation requests,  
10 for work with a funeral director or medical examiner, for certain lawsuits, legal actions, or law  
11 enforcement or government requests. The Data Breach met none of those exceptions.

12           72. Fred Hutch failed to live up to its own stated policies and promises with regards  
13 to data privacy and data security as cybercriminals were able to infiltrate its systems and steal  
14 the Private Information of Plaintiff and Class members.

15           73. Indeed, Fred Hutch’s website states that immediately following the Data Breach  
16 it conducted an investigation of the incident, “quarantined the servers,” and “implemented  
17 additional information technology security protocols.” This strongly implies that Fred Hutch’s  
18 security measures, by their own determination, were inadequate.<sup>37</sup>

19  
20  
21           <sup>34</sup> *Privacy Policy*, Fred Hutch Cancer Center, <https://www.fredhutch.org/en/util/patient-policies.html#public-policy> (last visited Dec. 7, 2023).

22           <sup>35</sup> *Joint Notice of Privacy Practices: Your Information. Your Rights. Our Responsibilities.*, Fred  
Hutch Cancer Center (Dec. 19, 2022), <https://www.fredhutch.org/content/dam/www/clinical-pdf/patient-policies/joint-notice-of-privacy-practices.pdf> (last visited Dec. 7, 2023).

23           <sup>36</sup> *Id.*

24           <sup>37</sup> *Update on Data Security Incident*, Fred Hutch Cancer Center,  
<https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html>  
(last visited Dec. 7, 2023).

**F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach**

74. Like any data breach, the Data Breach in this case presents major problems for all affected.<sup>38</sup>

75. The FTC warns the public to pay particular attention to how they keep PII, including Social Security numbers and other sensitive data. As the FTC notes, “once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”<sup>39</sup>

76. The ramifications of Fred Hutch’s failure to properly secure Plaintiff’s and Class members’ Private Information are severe. Identity theft occurs when someone uses another person’s financial, medical, or personal information, such as that person’s name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

77. PII has a long shelf-life because it can be used in more ways than one, and it typically takes time for an information breach to be detected.

78. Plaintiff and Class members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves, or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI and then risk prosecution by listing it for sale on the dark web if the PII and PHI was not valuable to malicious actors.

---

<sup>38</sup> Paige Schaffer, *Data Breaches’ Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at <https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers> (last accessed Dec. 7, 2023).

<sup>39</sup> *Warning Signs of Identity Theft*, Federal Trade Comm’n, available at <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed Dec. 7, 2023).

1           79.     The dark web helps ensure users' privacy by effectively hiding server or IP details  
 2 from the public. Users need special software to access the dark web. Most websites on the dark  
 3 web are not directly accessible via traditional searches on common search engines and are  
 4 therefore accessible only by users who know the addresses for those websites.

5           80.     Malicious actors use Private Information to gain access to Class members' digital  
 6 life, including bank accounts, social media, and credit card details. During that process, hackers  
 7 can harvest other sensitive data from the victim's accounts, including personal information of  
 8 family, friends, and colleagues.

9           81.     Consumers are injured every time their data is stolen and placed on the dark web,  
 10 even if they have been victims of previous data breaches. Not only is the likelihood of identity  
 11 theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete  
 12 repositories of stolen information. Each data breach puts victims at risk of having their  
 13 information uploaded to different dark web databases and viewed and used by different criminal  
 14 actors.

15           82.     Malicious actors can use Class members' Private Information to open new  
 16 financial accounts, open new utility accounts, obtain medical treatment using victims' health  
 17 insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or  
 18 create "synthetic identities."

19           83.     As established above, the PII accessed in the Data Breach is also very valuable to  
 20 Fred Hutch. Fred Hutch collects, retains, and uses this information to increase profits—it even  
 21 notes that it will use Class members' data for this reason without their written permission.<sup>40</sup> Fred  
 22

---

23           <sup>40</sup> See *Joint Notice of Privacy Practices: Your Information. Your Rights. Our Responsibilities.*,  
 24 Fred Hutch Cancer Center (Dec. 19, 2022), [https://www.fredhutch.org/content/dam/www/clinical-  
 pdf/patient-policies/joint-notice-of-privacy-practices.pdf](https://www.fredhutch.org/content/dam/www/clinical-pdf/patient-policies/joint-notice-of-privacy-practices.pdf) (last visited Dec. 7, 2023). (stating that patient

Hutch patients value the privacy of this information and expect Fred Hutch to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Fred Hutch, provided their PII and PHI, and/or paid the same prices for Fred Hutch's services had they known Fred Hutch did not implement reasonable security measures to protect their PII and PHI. Patients expect that the payments they make to the medical providers incorporate the costs to implement reasonable security measures to protect their Private Information.

84. The Private Information accessed in the Data Breach is also very valuable to Plaintiff and Class members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class members' PII has been compromised and lost significant value.

85. Plaintiffs and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections

---

information may be used to "run our practice," "improve care," or used in furtherance of its own "health research").

1 agencies. Plaintiffs and Class members will therefore need to continuously monitor their accounts  
2 for years to ensure their PII obtained in the Data Breach is not used to harm them.

3 86. Even when reimbursed for money stolen due to a data breach, consumers are not  
4 made whole because the reimbursement fails to compensate for the significant time and money  
5 required to repair the impact of the fraud.

6 87. Accordingly, Fred Hutch's wrongful actions and inaction and the resulting Data  
7 Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing  
8 increased risk of identity theft and identity fraud. According to a recent study published in the  
9 scholarly journal "Preventive Medicine Reports," public and corporate data breaches correlate to  
10 an increased risk of identity theft for victimized consumers.<sup>41</sup> The same study also found that  
11 identity theft is a deeply traumatic event for victims, with more than a quarter of victims still  
12 experiencing sleep problems, anxiety, and irritation even six months after the crime.<sup>42</sup>

13 88. There is also a high likelihood that significant identity fraud and identity theft has  
14 not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals  
15 may be exploited in the future; there is a concrete risk that the cybercriminals who now possess  
16 Class members' Private Information will do so at a later date or re-sell it.

17 89. Data breaches have also proven to be costly for affected organizations as well,  
18 with the average cost to resolve a data breach in 2023 at \$4.45 million.<sup>43</sup> The average cost to  
19

---

20 <sup>41</sup> David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and Protective Factors of Identity*  
21 *Theft Victimization in the United States*, Preventive Medicine Reports, Volume 17 (March 2020),  
22 available at <https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub> (last  
23 accessed Dec. 7, 2023).

24 <sup>42</sup> *Id.*

<sup>43</sup> *Cost of a Data Breach Report 2023*, IBM Security, available at  
[https://www.ibm.com/reports/data-breach?utm\\_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRINbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD\\_BwE&gclsrc=aw.ds](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRINbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds) (last accessed Dec. 7, 2023).

1 resolve a data breach involving health information, however, is more than double this figure at  
2 \$10.92 million.<sup>44</sup>

3 90. The theft of medical information, beyond the theft of more traditional forms of  
4 PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records  
5 and information, has seen a seven-fold increase over the last five years, and this explosive growth  
6 far outstrips the increase in incidence of traditional identity theft.<sup>45</sup> Medical identity theft is  
7 especially harmful for victims because of the lack of laws that limit a victim's liabilities and  
8 damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges  
9 is capped at \$50), the unalterable nature of medical information, the sheer costs involved in  
10 resolving the fallout from a medical identity theft (victims spend, on average, \$13,500 to resolve  
11 problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.<sup>46</sup>

12 91. Here, due to the Breach, Plaintiff and Class members have been exposed to  
13 injuries that include, but are not limited to:

- 14 a. Theft of Private Information;
- 15 b. Costs associated with the detection and prevention of identity theft and  
16 unauthorized use of financial accounts and health insurance information  
17 as a direct and proximate result of the Private Information stolen during  
18 the Data Breach;
- 19 c. Damages arising from the inability to use accounts that may have been  
20 compromised during the Data Breach;
- 21 d. Costs associated with spending time to address and mitigate the actual and  
22 future consequences of the Data Breach, such as finding fraudulent  
23 charges, purchasing credit monitoring and identity theft protection  
24 services, placing freezes and alerts on their credit reports, contacting their  
financial institutions to notify them that their personal information was

---

22 <sup>44</sup> *Id.*

23 <sup>45</sup> Medical Identity Theft, AARP (Mar. 25, 2022), *available at*  
<https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html> (last accessed Dec. 7,  
2023).

24 <sup>46</sup> *Id.*

exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, monitoring claims made against their health insurance, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; and

e. The loss of Plaintiff's and Class members' privacy.

92. Plaintiff and Class members have suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will continue for years and years. The unauthorized access of Plaintiff's and Class members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely.

93. As a direct and proximate result of Fred Hutch's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

94. In addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose Private Information was accessed in the Data Breach, Plaintiff retains an interest in ensuring there are no future breaches. On information and belief, Fred Hutch is still in possession, custody, or control of Plaintiff's and the Class members' Private Information.

#### **G. Experiences Specific to Plaintiff**

##### ***Jonathan Hunter's Experience***

95. Plaintiff Hunter is a recent patient of Fred Hutch Cancer Center/University of Washington.

1           96.     Mr. Hunter received an email from Fred Hutch about the Data Breach. The notice  
2 instructed him to “remain vigilant to protect against potential fraud and/or identity theft”  
3 implying that his Private Information may have been compromised in the breach.

4           97.     As a result of the Data Breach, Mr. Hunter has made reasonable efforts to mitigate  
5 the impact of the Data Breach, including, but not limited to, researching the Data Breach and  
6 reviewing his financial accounts. He has also spent several hours dealing with the Data Breach,  
7 valuable time he otherwise would have spent on other activities, including, but not limited to,  
8 recreation and rest.

9           98.     As a result of the Data Breach, Plaintiff Hunter has suffered anxiety due to the  
10 public dissemination of his personal information, which he believed would be protected from  
11 unauthorized access and disclosure, including anxiety about unauthorized parties viewing,  
12 selling, and using his private information for purposes of identity theft and fraud. Plaintiff Hunter  
13 is concerned about identity theft and fraud, as well as the consequences of such identity theft and  
14 fraud resulting from the Data Breach.

15           99.     Plaintiff Hunter suffered actual injury from having his Private Information  
16 compromised as a result of the Data Breach including, but not limited to (a) damage to and  
17 diminution in the value of his Private Information, a form of property that Fred Hutch obtained  
18 from her; (b) violation of his privacy rights; and (c) present, imminent and impending injury  
19 arising from the increased risk of identity theft and fraud.

20           100.    As a result of the Data Breach, Plaintiff Hunter anticipates spending considerable  
21 time and money on an ongoing basis to continue monitoring his accounts and to try to mitigate  
22 and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a  
23 present risk and will continue to be at increased risk of identity theft and fraud for years to come.  
24

1                                   **V.     CLASS REPRESENTATION ALLEGATIONS**

2           101.   Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P.  
3 23, a Class defined as:

4                       All persons in the United States whose Private Information was accessed  
5 in the Data Breach (the “Class”).

6 Excluded from the Class are Fred Hutch, its executives and officers, and the Judge(s) assigned  
7 to this case. Plaintiff reserves the right to modify, change or expand the Class definition after  
8 conducting discovery.

9           102.   In the alternative, Plaintiff brings this action on behalf of himself and, pursuant to  
10 Fed. R. Civ. P. 23, a subclass of:

11                     All persons who are residents of the State of Washington whose Private  
12 Information was accessed in the Data Breach (the “Washington  
Subclass”).

13 Excluded from the Washington Subclass are Fred Hutch, its executives and officers, and the  
14 Judge(s) assigned to this case.

15           103.   Numerosity: Upon information and belief, the Class is so numerous that joinder  
16 of all members is impracticable. Reports suggest that the number of affected individuals may be  
17 as high as 800,000.<sup>47</sup> The exact number and identities of individual members of the Class are  
18 unknown at this time, such information being in the sole possession of Fred Hutch and obtainable  
19 by Plaintiffs only through the discovery process. The members of the Class will be identifiable  
20 through information and records in Fred Hutch’s possession, custody, and control.

21  
22  
23                     <sup>47</sup> See Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch*  
24 *cyberattack*, KUOW (Dec. 6, 2023), <https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack> (last visited Dec. 7, 2023).

1           104. Existence and Predominance of Common Questions of Fact and Law: Common  
 2 questions of law and fact exist as to all members of the Class. These questions predominate over  
 3 the questions affecting individual Class members. These common legal and factual questions  
 4 include, but are not limited to:

- 5           a. When Fred Hutch learned of the Data Breach;
- 6           b. Whether cybercriminals obtained Class members' Private Information in  
 7 the Data Breach;
- 8           c. Whether Fred Hutch's response to the Data Breach was adequate;
- 9           d. Whether Fred Hutch failed to implement and maintain reasonable security  
 10 procedures and practices appropriate to the nature and scope of the Private  
 11 Information compromised in the Data Breach;
- 12           e. Whether Fred Hutch's data security systems prior to and during the Data  
 13 Breach complied with applicable data security laws and regulations,  
 14 industry standards, and/or its own promises and representations;
- 15           f. Whether Fred Hutch knew or should have known that its data security  
 16 systems and monitoring processes were deficient;
- 17           g. Whether Fred Hutch owed a duty to Class members to safeguard their  
 18 Private Information;
- 19           h. Whether Fred Hutch breached its duty to Class members to safeguard their  
 20 Private Information;
- 21           i. Whether Fred Hutch had a legal duty to provide timely and accurate notice  
 22 of the Data Breach to Plaintiff and the Class members;
- 23           j. Whether Fred Hutch breached its duty to provide timely and accurate  
 24 notice of the Data Breach to Plaintiff and Class members;
- k. Whether Fred Hutch's conduct violated the FTCA, HIPAA, and/or the  
 Consumer Protection Act invoked herein;
- l. Whether Fred Hutch's conduct was negligent;
- m. Whether Fred Hutch was unjustly enriched;

- n. What damages Plaintiff and Class members suffered as a result of Fred Hutch's misconduct;
- o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;
- p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and
- q. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

105. Typicality: All of Plaintiff's claims are typical of the claims of the Class. Upon information and belief, Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Fred Hutch's uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Fred Hutch has acted, and refused to act, on grounds generally applicable to the Class.

106. Adequacy: Plaintiff is an adequate class representative because his interests do not materially or irreconcilably conflict with the interests of the Class he seeks to represent, he retained counsel competent and highly experienced in complex class action litigation, and he intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

107. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Fred Hutch's conduct. It would be virtually impossible for members of the Class individually to

effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on Fred Hutch's records and databases.

## **VI. CLAIMS FOR RELIEF**

### **COUNT I NEGLIGENCE**

**(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)**

108. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

109. Fred Hutch owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Fred Hutch also owes several specific duties including, but not limited to, the duty:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;
- d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;
- e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

1 f. to promptly notify Plaintiff and Class members of the Data Breach, and to  
2 precisely disclose the type(s) of information compromised.

3 110. Fred Hutch also owes this duty because Section 5 of the Federal Trade  
4 Commission Act, 15 U.S.C. § 45 requires Fred Hutch to use reasonable measures to protect  
5 confidential data.

6 111. Fred Hutch also owes this duty because industry standards mandate that Fred  
7 Hutch protect its patients' confidential Private Information.

8 112. Fred Hutch also owes this duty because it had a special relationship with Plaintiff  
9 and Class members. Plaintiff and Class members entrusted their Private Information to Fred  
10 Hutch on the understanding that adequate security precautions would be taken to protect this  
11 information. Furthermore, only Fred Hutch had the ability to protect its systems and the Private  
12 Information stored on them from attack.

13 113. Fred Hutch also owes a duty to timely disclose any unauthorized access and/or  
14 theft of the Private Information belonging to Plaintiff and the Class. This duty exists to allow  
15 Plaintiff and the Class the opportunity to undertake appropriate measures to mitigate damages,  
16 protect against adverse consequences, and thwart future misuse of their Private Information.

17 114. Fred Hutch breached its duties to Plaintiff and the Class by failing to take  
18 reasonable appropriate measures to secure, protect, and otherwise safeguard the Private  
19 Information belonging to Plaintiff and Class members.

20 115. Fred Hutch also breached the duties it owed to Plaintiff and the Class by failing  
21 to timely and accurately disclose to Plaintiff and Class members that their Private Information  
22 had been improperly acquired and accessed.

116. As a direct and proximate result of Fred Hutch's conduct, Plaintiff and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Permanent increased risk of identity theft.

117. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Fred Hutch, and the damages they suffered were the foreseeable result of Fred Hutch's inadequate security practices.

118. In failing to provide prompt and adequate individual notice of the Data Breach, Fred Hutch also acted with reckless disregard for the rights of Plaintiff and Class Members.

119. Plaintiff is entitled to damages in an amount to be proven at trial and injunctive relief requiring Fred Hutch to, among other things, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

**COUNT II**  
**BREACH OF IMPLIED CONTRACT**  
**(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)**

120. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

121. Plaintiff and the Class provided Fred Hutch with their Private Information.

1           122. By providing their Private Information, and upon Fred Hutch's acceptance of this  
2 information, Plaintiff and the Class, on one hand, and Fred Hutch, on the other hand, entered into  
3 implied-in-fact contracts for the provision of data security, separate and apart from any express  
4 contract entered into between the parties.

5           123. The implied contracts between Fred Hutch and Plaintiff and Class members  
6 obligated Fred Hutch to take reasonable steps to secure, protect, safeguard, and keep confidential  
7 Plaintiff's and Class members' Private Information. The terms of these implied contracts are  
8 described in federal laws, state laws, and industry standards, as alleged above. Fred Hutch  
9 expressly adopted and assented to these terms in its public statements, representations and  
10 promises as described above.

11           124. The implied contracts for data security also obligated Fred Hutch to provide  
12 Plaintiff and Class members with prompt, timely, and sufficient notice of any and all  
13 unauthorized access or theft of their Private Information.

14           125. Fred Hutch breached these implied contracts by failing to take, develop and  
15 implement adequate policies and procedures to safeguard, protect, and secure the Private  
16 Information belonging to Plaintiff and Class members; allowing unauthorized persons to access  
17 Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and  
18 sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

19           126. As a direct and proximate result of Fred Hutch's breaches of the implied contracts,  
20 Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as  
21 detailed above due to the continued risk of exposure of Private Information, and are entitled to  
22 damages in an amount to be proven at trial.

**COUNT III  
UNJUST ENRICHMENT**

**(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)**

127. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

128. This count is brought in the alternative to Count II.

129. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Fred Hutch.

130. Fred Hutch was benefitted by the conferral upon it of Plaintiff's and Class members' Private Information and by its ability to retain and use that information. Fred Hutch understood that it was in fact so benefitted.

131. Fred Hutch also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential, and its value depended upon Fred Hutch maintaining the privacy and confidentiality of that information.

132. But for Fred Hutch's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Fred Hutch, and Fred Hutch would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiff and Class members, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise, and realizing excessive profits.

1           133. As a result of Fred Hutch's wrongful conduct as alleged herein (including, among  
2 other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope  
3 of the data breach; its failure to employ adequate data security measures; its continued  
4 maintenance and use of the Private Information belonging to Plaintiff and Class members without  
5 having adequate data security measures; and its other conduct facilitating the theft of that Private  
6 Information), Fred Hutch has been unjustly enriched at the expense of, and to the detriment of,  
7 Plaintiff and the Class.

8           134. Fred Hutch's unjust enrichment is traceable to, and resulted directly and  
9 proximately from, the conduct alleged herein, including the compiling and use of Plaintiff and  
10 Class members' sensitive Private Information, while at the same time failing to maintain that  
11 information secure from intrusion.

12           135. Under the common law doctrine of unjust enrichment, it is inequitable for Fred  
13 Hutch to be permitted to retain the benefits it received, and is still receiving, without justification,  
14 from Plaintiff and the Class in an unfair and unconscionable manner.

15           136. The benefit conferred upon, received, and enjoyed by Fred Hutch was not  
16 conferred officiously or gratuitously, and it would be inequitable and unjust for Fred Hutch to  
17 retain the benefit.

18           137. Fred Hutch is therefore liable to Plaintiff and the Class for restitution in the  
19 amount of the benefit conferred on Fred Hutch as a result of its wrongful conduct, including  
20 specifically the value to Fred Hutch of the PII and medical information that was accessed and  
21 exfiltrated in the Data Breach and the profits Fred Hutch receives from the use and sale of that  
22 information.

138. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Fred Hutch and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Fred Hutch from its wrongful conduct.

139. Plaintiff and Class Members may not have an adequate remedy at law against Fred Hutch, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT IV**  
**VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT**  
**Wash. Rev. Code § 19.86.020, *et seq.***  
**(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)**

140. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

141. Plaintiff and Class members are “persons” under the Washington Consumer Protection Act. RCW 19.86.010(1).

142. Defendant is a “person” as described in the Washington Consumer Protection Act. RCW 19.86.010(1).

143. Fred Hutch is engaged in, and its acts and omissions affect, trade and commerce. Fred Hutch’s relevant acts, practices, and omissions complained of in this action were done in the course of Fred Hutch’s business of marketing, offering for sale, and selling services throughout Washington and the United States.

144. Fred Hutch is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and many of its employees are residents of the State of Washington.

1           145. The Washington Consumer Protection Act prohibits deceptive and unfair acts or  
2 practices in the conduct of any business, trade, or commerce, or in the provision of commerce.  
3 RCW 19.86.020.

4           146. In the course of conducting its business, Fred Hutch committed “unfair acts or  
5 practices” by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee,  
6 manage, monitor and audit appropriate data security processes, controls, policies, procedures,  
7 protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class  
8 Members’ Private Information. Such practices were likely to cause substantial injury to  
9 consumers and were, not reasonably avoidable by consumers and nor outweighed by  
10 countervailing benefits.

11           147. Fred Hutch’s conduct was also deceptive. Fred Hutch failed to timely notify and  
12 concealed from Plaintiff and Class Members the inadequacy of its data security measures and the  
13 unauthorized release and disclosure of their Private Information. If Plaintiff and Class Members  
14 had been notified in an appropriate fashion, and had the information not been hidden from them,  
15 they could have taken precautions to safeguard and protect their Private Information, medical  
16 information, and identities.

17           148. Fred Hutch’s unfair and deceptive acts or practices in the conduct of business  
18 include, but are not limited to:

- 19           a. Failing to implement and maintain reasonable security and privacy  
20 measures to protect Plaintiff’s and Class members’ Private Information,  
which was a direct and proximate cause of the Data Breach;
- 21           b. Failing to identify foreseeable security and privacy risks, remediate  
22 identified security and privacy risks, and adequately improve security and  
privacy measures following previous cybersecurity incidents in the  
23 industry, which were direct and proximate causes of the Data Breach;
- 24           c. Failing to comply with common law and statutory duties pertaining to the  
security and privacy of Plaintiff’s and Class members’ Private

Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information;
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information; and
- h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

149. Fred Hutch's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

150. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should or could have reasonably avoided.

151. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct and proximate result of Fred Hutch's unfair and deceptive acts and practices as set forth herein include, without limitation:

- a. theft of their Private Information;
- b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and health insurance;

- c. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- e. damages to and diminution in value of their Private Information entrusted to Fred Hutch, and with the understanding that it would safeguard their data against theft and not allow access and misuse of their data by others; and
- f. the continued risk to their Private Information, which remains in the possession of Fred Hutch and which is subject to further breaches so long as it fails to undertake appropriate and adequate measures to protect data in its possession.

152. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Fred Hutch from disclosing their Private Information without their consent and prohibiting Fred Hutch from continuing its wrongful conduct; reasonable attorneys' fees and costs; treble damages for each Class member, not to exceed \$25,000 per Class member; and any other relief that is just and proper under RCW 19.86.090.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Fred Hutch, as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to CR 23; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
- B. That Plaintiff be granted the declaratory relief sought herein;

- C. That the Court grant permanent injunctive relief to prohibit Fred Hutch from continuing to engage in the unlawful acts, omissions, and practices described herein;
- D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- E. That the Court award Plaintiff and the Class members statutory damages, and treble damages, to the extent permitted by law;
- F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- G. That the Court award pre- and post-judgment interest at the maximum legal rate;
- H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution;
- I. That the Court grant leave to amend these pleadings to conform to evidence produced at trial; and
- J. That the Court grant all other relief as it deems just and proper.

# **JURY DEMAND**

Plaintiff demands a trial by jury.

Date: December 26, 2023

Respectfully Submitted,

# **TOUSLEY BRAIN STEPHENS PLLC**

s/ Kim D. Stephens, P.S.

Kim D. Stephens, P.S., WSBA #11984

s/ Cecily C. Jordan

Cecily C. Jordan, WSBA #50061

1200 Fifth Avenue, Suite 1700

Seattle, WA 98101

Telephone: 206-682-5600

Facsimile: 206-682-2992

kstephens@tousley.com

cjordan@tousley.com

James J. Pizzirusso\*

HAUSFELD LLP

888 16th Street N.W.

Suite 300

Washington, D.C. 20006

(202) 540-7200

jpizzirusso@hausfeld.com

1 Steven M. Nathan\*  
2 HAUSFELD LLP  
3 33 Whitehall Street  
4 Fourteenth Floor  
5 New York, NY 10004  
6 (646) 357-1100  
7 snathan@hausfeld.com

8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
*Attorneys for Plaintiff and the Proposed Class*

*\* Pro Hac Vice Forthcoming*